「国民生活研究」第 61 巻第 2 号（2021 年 12 月）
【特集】キャッシュレスの現在と未来
［論　文］

各種のキャッシュレス支払いと消費者保護

小　塚　荘一郎*

Ⅰ　キャッシュレス支払いの類型
Ⅱ　不正使用（無権限取引）のリスク
Ⅲ　銀行預金を決済手段とするキャッシュレス取引の消費者リスク
Ⅳ　電子データを決済手段とする支払いシステムの消費者リスク
Ⅴ　無権限取引のまとめ
Ⅵ　結語

Ⅰ　キャッシュレス支払いの類型

1　本稿の目的

キャッシュレス社会の実現という政策目標は、平成 28 年に、『日本再興戦略 2016』（いわゆる「骨太の方針」）に初めて盛り込まれた。それ以来５年の間に、さまざまな支払い手段が出現し、キャッシュレスの支払いは、一般の消費者にも身近なものとなっている[1)]。しかし、使い慣れたように思われる支払い手段でも、ひとたびトラブルが発生すると、消費者にはどのような権利があり、どのようにして救済を受けられるのかはわからないという場合も少なくない。そうしたことが繰り返されると、キャッシュレス支払いに対する消費者の信頼が失われ、ひいては、その普及にブレーキがかかることになりかねない。そのため、キャッシュレス支払いの仕組みを正しく理解した上で、その利用において発生するリスクが利用者（消費者）とその他の関係者の間でどのように分配されているかを明らかにすることは重要である。

＊こづか そういちろう（学習院大学法学部 教授）

本稿は、このような問題意識から、キャッシュレス支払いの類型ごとに、現在の法制度や判例の下でとられているリスクの分配について整理したものである。なお、以下の記述の中では、キャッシュレス支払いの「利用者」と「消費者」を区別していない。もちろん、利用者が法律上の「消費者」の定義に該当する場合、利用者と支払いシステムの提供主体との契約に消費者契約法が適用されるといった相違がある。しかし、一般的に、「キャッシュレス支払い」は企業間取引でのみ用いられる支払い決済システム（電子記録債権やグループ企業間の CMS（cash management system）など）を含まない意味で用いられている。そしてそのように定義された「キャッシュレス支払い」については、利用者の属性によってリスク分配のルールに差を設ける合理性が乏しいと考えられるので、少なくとも基本的な考え方を整理する上では、利用者が「消費者」であるか否かを区別する必要はないと考える。

2　支払いシステムと決済

消費者から見ると、キャッシュレスは「支払い」の場面で問題になる。「支払い」（payment）とは、わかりやすく言えば、なんらかの取引に対して「お金を払う」ことである。それを法律的に説明すれば、原因取引から発生する金銭債務の弁済ということになる。

しかし、どのような「支払い」の仕組みも、その背後で「決済」（settlement）の仕組みが動かなければ、意味を持たない[2)]。支払いが金銭債務の弁済行為である以上、最終的に、債権者に対する金銭の提供という結果が実現されなければならないからである。消費者が、こうした「支払い」と「決済」の関係を意識することが少ない理由は、現金による支払いを無意識のうちに基準として考えているためであろう。現金については「占有と所有が一致する」と言われ[3)]、たとえ盗んできた貨幣を使って支払っても、有効な支払いになる。後になって、盗まれた紙幣が番号から特定されても、それを受け取った商店から紙幣が犯罪組成物品として取り上げられることはない。このような点で、現金はきわめて特殊な支払い手段であり、例外的に、決済の仕組みを必要としないのである。

現金以外の支払い手段については、支払いと決済の仕組みを総体として理解する必要がある。キャッシュレス支払いのうち、クレジットカードやデビットカードは、銀行預金を消費者から加盟店に付け替えることで決済が実行される。ここで決済の媒体を「決済手段」と呼ぶことにするならば、これらは、銀行預金を決済手段とする支払い手段である。

それに対して、従来から日本で普及していた IC カード型の電子マネー（とくに交通系）は、銀行預金の付け替えで決済を行う仕組みとはなっていない。加盟店に対しては、電子マネーの発行会社が残高を買いとる形になっているので、残高相当額（消費者からの支払いの合計額）が加盟店の銀行預金に振り込まれることになるが、カード保有者の側は、現金でチャージしている場合も多い。クレジットカードと一体化してオートチャージしている場合にも、カード保有者の銀行預金口座から直接に、加盟店の銀行預金口座へと預金の付け替え（振込または振替）が行われるわけではない。この場合、支払いの当事者間における決済手段は銀行預金ではなく、電子データであると言うほかはないように思われる。

電子データを決済手段とするキャッシュレスの仕組みは、日本の消費者が慣れ親しんだ

現金による支払いを、デジタルの世界で忠実に再現しようとしたものであろう。そして、そのゆえに広く普及したと考えられる。これに対して、銀行預金を決済手段とするキャッシュレス支払いは、これまで日本では限定的にしか使われず、そのことが、日本におけるキャッシュレス支払いが遅れていると言われる一因になっていた。

QR コード支払いをはじめとする近年の新しいキャッシュレス支払い（マスメディアで「キャッシュレス決済」と呼ばれているが、以上の点をふまえればキャッシュレス「支払い」と言うべきである）は、銀行口座からの引き落としや ATM による現金の入金、クレジットカードによる支払い等の方法でチャージすることが基本となっているが、一部のクレジットカードから直接支払いを行う方法も選択できるものがある。これは、一次的な支払い手段（クレジットカードや現金チャージによる電子マネー）を複数統合して、二次的な支払い手段を作り出し、その結果として、消費者の利便性が高められたものということができよう。決済のシステムとして見ると、いったんチャージが行われるときは、実際に残高が使われるよりも前にチャージ元の銀行預金から引き落としがなされるので、決済手段は銀行預金ではなく、電子データであると考えられる（IC カードへのオートチャージと同じである）。それに対して、支払いの時点でクレジットカードから直接の支払いがなされるのであれば、クレジットカードを使用した支払いと変わらず、銀行預金を決済手段とした支払いになる。すなわち、一つの支払い手段に対して、決済手段が複数存在するという関係になっているわけである。

Ⅱ　不正使用（無権限取引）のリスク

以上のような理解をふまえた上で、キャッシュレス取引における消費者のリスクについて考えてみよう。消費者がキャッシュレス支払いについて抱く不満の中には、原因取引にかかわるもの（悪質な取引であったにもかかわらず支払いが実行されてしまう等）もあるが、ここでは、支払いシステムに固有のリスクとして、「不正使用」を考える。

支払いシステムの「不正使用」と呼ばれる問題の中にも、二つの類型を区別した方がよい。一つは、名義上の利用者（名義人）ではない者が支払いを実行してしまうこと、法的に言えば、無権限者による支払いシステムの利用である。それによって、名義人から使用できたはずの残高が奪われ、別の何者かが、商品・サービスを購入して利益を得る。この類型の特徴は、不正に使われたと言っても支払い手段それ自体は真正のものであり、それを使用する権限の主体、くだけた言い方をすれば「持ち主」がすり替えられているという点にある。

同じく「不正使用」と呼ばれても、これと区別される類型は、システムがハッキング等により攻撃され、データが書き換えられるというものである。データの書き換えによって、たとえば残高が不正に増額され、本来存在してはならない支払い手段が作り出されてしまった場合には、直接の被害者は存在しない。しかし、支払いシステム全体としては、裏づけのない支払い手段が有効なものとして使用されるという損失を被ることになる。他方で、残高が不正に消されるタイプの書き換えもあり得るが、この場合は、被害者は存在するに

もかかわらず利得する者は誰もいないという不思議な状況が出現する（消された残高を何者かが使っていれば、ここでいう「データの書き換え」ではなく、「無権限者による利用」である）。

データの書き換えという後者の類型の処理について考えると、直接的な被害者が存在しないデータの不正増額のケースでは、システム運営者がそのコストを負担するという以外の解決は難しいであろう。不正に作り出された支払い手段と、正規の支払い手段とをシステム上で区別することは、貨幣や紙幣の偽造であればまだしも、デジタル技術を前提とするキャッシュレス取引ではほとんど考えられないからである。これに対して、データの不正抹消の場合、被害者を放置するという選択をしないのであれば、システム運営者から被害者に補償することが、ほぼ唯一の現実的な選択肢である（データの不正な操作を行った者に不法行為による損害賠償等を請求することはできる）。さらに言えば、そうした攻撃を防ぐためにはコストをかけてシステムのセキュリティを強化しなければならないが、それらの負担やコストもまた、システム運営者の負担になる。

システム運営者が負担するこれらのコストは、消費者にとって、無償のものではない。いずれの場合も、システム運営者は、こうした負担を運営コストとして、消費者や加盟店という支払いシステムの利用者に対し、手数料・利用料として転嫁するであろう。保険を利用すれば解決するという意見が聞かれることもあるが、保険市場が正常に機能しているならば、リスクに見合った保険料を支払う必要が生ずるので、保険料がシステム運営のコストとなり、消費者や加盟店への転嫁が発生することに変わりはない。結局のところ、支払いシステムが不正利用されるリスクは、システムの利用者が、利用のコストとして「広く薄く」負担するのである。

無権限者による支払いの実行という類型の場合にも、これと同じ解決を図ることが考えられる。被害を受けた名義人に対しては、支払いシステムの負担において被害発生前の状態を回復させつつ、無権限者から支払いを受けた加盟店との関係では支払いの有効性を承認するという方法である。後述するとおり、銀行キャッシュカードやクレジットカードの盗難による不正利用については、一定の要件の下で、こうした解決がとられている。このような制度が採用されると、面倒な手続の負担などを度外視すれば（実際にはこの部分の負担も大きいのであるが）、消費者にとって、無権限者による利用のリスクは解消する。しかし、その場合も、支払いシステムを全体として見たときのリスクが消滅するわけではない。消費者にとってのリスクを解消するために要した費用は、支払いシステム利用のコストとなって、キャッシュレス支払いシステムの利用料・手数料などを通じ、すべての消費者と加盟店に「広く薄く」転嫁されるであろう。

しかし、無権限取引の場合には、支払いシステムが全体として負担するという方法のほかに、加盟店（債権者）にリスクを負わせる（無権限の支払いを無効として、代金債権が未払いの状態に戻す）方法や、逆に、名義人にリスクを負わせる（無権限の支払いによる残高の費消を有効とする）方法が取られる場合もある。その理由は、加盟店や名義人がなんらかの行動をとることによって、無権限取引が行われるリスクを抑制する可能性があるためである。

そもそも、キャッシュレス支払いが消費者の信頼を得るためには、トラブルが発生するリスクを減らさなければならない。リスクを放置したまま、対症療法的に個別の事案で消費者を満足させたとしても、キャッシュレス支払いに対する信頼にはつながらないであろう。そして、もっぱら技術的な問題に起因するデータの不正な書き換えとは異なり、無権限の取引リスクは、名義人や加盟店の行動によって抑制する余地も大きい。極端な場合には、それらの当事者が不正に加担していることすらある。このとき、一定の範囲で当事者にリスクを負担させるという制度を採用すると、そのことを通じて、名義人や加盟店にリスクを抑制するような行動をとるインセンティヴが生まれ、結果的には支払いシステム全体にとって望ましい状態が実現される可能性がある。そうした制度設計を考える際には、それぞれの支払いシステムの仕組みを正しく理解した上で、どこに、どのようなリスクが存在するかを把握し、それをふまえて、誰が、どのような行動をとるとリスクを抑制できるかを考えることが重要になる。

Ⅲ　銀行預金を決済手段とするキャッシュレス取引の消費者リスク

1　機械による預金の払い出しと免責規定

キャッシュレス支払いにおける不正使用については、通常、システム利用契約（約款）に、そのリスク負担に関する規定が置かれている。そして、その規定を適用した結果に不満があれば、規定の有効性を争うことになる。システムの運営者がリスクを負担する場合に、あえてその有効性を争う利用者はいないと思われるので、裁判例に現れる事案は、約款の規定によってシステム運営者が免責され、リスクが利用者の負担とされる場合である。

このとき、裁判所は、システムの運営者が免責されるためには、システムに相当な水準の安全性が具備されていることが前提となると解している。このような考え方は、機械を通じた預金の払い出しをめぐる事案を通じて発展してきた。そこで、キャッシュレス取引そのものではないが、預金払い出しに関する裁判例の検討から始めよう。

最初に現れた事例は、銀行キャッシュカードが、カードの名義人以外の者により現金自動支払機（CD 機）で使用され、預金が払い出されたという事案に関するものであった。最高裁は以下のように判示し、暗証番号管理の不備を例として挙げながら、「特段の事情」により免責約款の効力が否定される可能性を明確に認めた（［A］最判平成５・７・19 判例時報 1489 号 111 頁）。

> 「銀行の設置した現金自動支払機を利用して預金者以外の者が預金の払戻しを受けたとしても、銀行が預金者に交付していた真正なキャッシュカードが使用され、正しい暗証番号が入力されていた場合には、銀行による暗証番号の管理が不十分であったなど特段の事情がない限り、銀行は、現金自動支払機によりキャッシュカードと暗証番号を確認して預金の払戻しをした場合には責任を負わない旨の免責約款により免責されるものと解するのが相当である。」

ただし、結論としては、この事案では免責の有効性を否定すべき「特段の事情」はなかったとされている。当時（無権限者による払い出しの発生は昭和 56 年）、銀行キャッシュカードの磁気ストライプ上には、暗証番号がコード化された状態で記録されており、原告（預金者）は、「市販のカードリーダーをパソコンに接続すれば、簡単に暗証番号を知り、コピーを作り、あるいはコードを変更したカードを作ることができるようになる」と主張した（［A］の一審判決である東京地判平成元・１・31 判例時報 1310 号 105 頁参照）。しかし、最高裁は、「所論の方法で暗証番号を解読するためにはコンピューターに関する相応の知識と技術が必要であることは明らかである（なお、記録によれば、本件支払がされた当時、このような解読技術はそれほど知られていなかったことがうかがえる。）から、被上告人が当時採用していた現金自動支払機による支払システムが免責約款の効力を否定しなければならないほど安全性を欠くものということはでき［ない］」と判断した。これは、キャッシュカードの安全性が確保されていないという預金者の主張に対して、それを免責条項の有効性が認められなくなる「特段の事情」の問題と位置づけた上で、事案の中で具体的に判断したものということができよう。

セキュリティを免責条項の前提条件とする解釈は、この判決以前から、学説によって示唆されていたものである。そうした学説の中には、セキュリティの確保を、機械払いによる弁済を行う金融機関の付随的義務と位置づける可能性を示唆するものもあった[4]。しかし、本判決は、約款の条項に従った免責が認められない「特段の事情」の例に暗証番号管理の不備を挙げているので、契約当事者の合理的な意思として、システム運営者としてのセキュリティ確保義務が果たされない場合にまで金融機関に免責を与える趣旨ではないと解釈したのではないかと思われる[5]。

２　債務者の過失とシステムの安全性

その後、最高裁は、民法 478 条の解釈としても、金融機関が預金債権の債務者として免責されるためにはシステムのセキュリティが前提になるという解釈を示した。判決の事案は、預金者が自動車のダッシュボードに預金通帳を入れたまま自動車を盗まれたところ、何者かによって現金自動入出機（ATM）から預金が払い出されたというものであった。この銀行では、預金通帳と暗証番号の組み合わせにより機械払いを受けることができるというシステムがとられており、本件では暗証番号が自動車の車両ナンバーであったため、自動車を盗んだ者に見破られてしまったようである。預金規定には通帳と印鑑を用いた払い出しに関する免責条項があり、カード規定にはキャッシュカードと暗証番号による払い出しについての免責条項が置かれているが、通帳と暗証番号の組み合わせによる機械払いについての免責条項は、どの規定にも存在していなかったため、裁判所は、民法 478 条の適用によって払い出しの有効性を判断することになった。最高裁は、次のように述べている（［B］最判平成 15・４・８民集 57 巻４号 337 頁）。

「債権の準占有者に対する弁済が民法 478 条により有効とされるのは弁済者が善意かつ無過失の場合に限られるところ、債権の準占有者に対する機械払の方法による預金の

払戻しにつき銀行が無過失であるというためには、払戻しの際に機械が正しく作動したことだけでなく、銀行において、預金者による暗証番号等の管理に遺漏がないようにさせるため当該機械払の方法により預金の払戻しが受けられる旨を預金者に明示すること等を含め、機械払システムの設置管理の全体について、可能な限度で無権限者による払戻しを排除し得るよう注意義務を尽くしていたことを要する」

民法 478 条の特徴は、債権者（消費者）の側の帰責事由を問題とせず、債務者側の過失のみによって弁済の有効性を判断する点にあると言われる[6)]。最高裁は、この「無過失」の要件にシステムの安全性（セキュリティ）を読み込んだわけである。しかも、そこにいうセキュリティは、技術的、物理的な安全性を言うだけではなく、リスクの周知も含め、無権限者による不正利用のリスクを最小化する措置を広く含むとした。製造物責任における「欠陥」は、設計上の欠陥、製造上の欠陥だけではなく指示・警告上の欠陥をも含むとされているが、そのことを想起させる判示である。

無権限の預金払い出しに関するこうした判例の考え方は、以下に述べるとおり、無権限のオンライン振込や仮想通貨（暗号資産）の使用などの事案にも応用され、キャッシュレス取引に関する基本的な考え方となっている。現行民法の下では、定型約款の拘束力を判断する際に、信義則に反して相手方の利益を一方的に害する条項であるか否かが基準となるが（民法 548 条の２第２項）、仮に、システムの安全性にかかわらず支払いシステム運営者の免責を認めるような条項が定型約款に含まれていたとすれば、民法 478 条に関する判例の考え方に照らし、この基準に照らして拘束力が否定される可能性が高いであろう。

３　偽造カード法によるリスク負担の修正

最高裁の［A］・［B］両判決は理論的に重要な判例であるが、無権限者によるキャッシュカードの使用については、平成 17 年に「偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律」（偽造カード法）が制定されたため、直接に民法 478 条が適用される場面はほとんどなくなっている。この法律は、そもそも正規に発行されてはいない「偽造カード」と、真正なカードが盗まれて不正使用された「盗難カード」を区別した上で、民法 478 条（およびその解釈を前提とした免責条項の有効性）にもとづくリスク分配を修正した法律である。前述のとおり、無権限者による不正取引とデータの不正な書き換えとではリスクとしての性質が異なる。偽造カード法は、この区別を正当に認識し、それに対応した制度の作り方であると言える。

偽造カードを機械（ATM）で使用した無権限の払い出しについては、民法 478 条を排除して独自のリスク分配ルールが定められた（偽造カード法３条）。これに対して、盗難カードを機械（ATM）で使用した無権限の払い出しについて、民法 478 条を適用した結果を銀行による「補てん」という形で修正するものとしている。いずれについても預金者の側の事情をもリスク分配の基準として参照する点と、盗難カードの不正使用については「補てん」という仕組みを利用することで、預金の消滅か全額保護かのオール・オア・ナッシングではなく、中間的な解決をも認めた点が、民法 478 条と異なる特徴である。

まず、偽造カードによる預金払い出しの場合は、①預金者に故意がある場合（偽造カードの作成者に暗証番号等を教えた場合などが該当するであろう）と、②金融機関側が善意無過失であって、かつ預金者に重大な過失がある場合に限って、預金の払い出しが有効となり、預金者がリスクを負担する（偽造カード法４条１項）。偽造カードが作成されるという事態は、通常、預金者自身が関与しない外在的なリスクである反面、金融機関側は、システム全体のセキュリティを強化することで偽造カードが使用される可能性を抑えられるので、リスクを生み出した主な原因が預金者側にある①や②の場合を除いて、金融機関側がリスクを負担すべきものとされたものと解される。

これに対して、盗難カードの不正使用については、民法 478 条が適用される（偽造カード法３条但書き。従って、同条に関する判例法も維持される）。そのことを前提として、一定の条件が満たされる場合には、金融機関が、払い出された預金額の一定割合を補てんするものとされる。補てんされる割合は金融機関および預金者の事情と相関しており、預金者が無過失ならば、カードの盗難を金融機関に対して速やかに通知し、かつ盗難に関する状況の説明を行うことを条件として全額の補てんを受けられる（預金者のリスク負担はゼロ）。金融機関が善意無過失であって預金者に過失があるときの補てんは払い出された金額の３／４のみ（預金者のリスク負担割合は 25%）、預金者に故意または重大な過失があるとき、預金者の同居の親族などによる払戻しのとき、および預金者が銀行に対して偽りの説明を行ったときと、戦争、暴動等による著しい社会秩序の混乱に際して盗難が発生したときは、補てんは行われない（預金者が 100%のリスク負担）、とされている（偽造カード法５条）。

これは、「著しい社会秩序の混乱」に起因するリスクを除けば、預金者側で可能なリスク管理と金融機関側に求められるリスク管理の双方に対してインセンティヴを設定した制度と見ることができる。そのようなとらえ方を前提とすれば、どのような事情が預金者側の「過失」や「重大な過失」として評価されるかについても、預金者に期待されるリスク管理行動は何かという観点から考えられるべきことになろう。平成 17 年に全国銀行協会が公表した「偽造・盗難キャッシュカードに関する預金者保護の申し合わせ」では、①本人が他人に暗証を知らせたとき、本人が暗証をキャッシュカードに書いたとき、本人が他人にキャッシュカードを渡したときなどは「重大な過失」となり得ること、②生年月日等を暗証番号とし、それを推測させる書類をキャッシュカードとともに携行したとき、暗証をメモに書いてキャッシュカードとともに携行したときなどは「過失」となり得ること、が了解されている[7]。預金者はカードと暗証番号の適切な管理を求められている（偽造カード法９条４項）という前提の下では、裁判所が、①に掲げられた行為を預金者の重大な過失に該当しないと判断する可能性は限られるであろう[8]。他方で、金融機関を代表する業界団体がこのような申し合わせを公表した以上は、金融機関はそれに従って事案を処理するであろうし、預金者の側から、これよりも預金者にとって厳しい取扱いをあえて求めることは考えられない。すると結局、申し合わせの内容が、偽造カード法の下で適用されるリスク分配のルールになると言える。

預金者側に帰責事由がない偽造・盗難リスクについて、「補てん」をも活用しつつ金融機

関の負担とする偽造カード法のリスク分配は、支払いシステムの運営者に対してシステムのセキュリティを向上させるインセンティヴを与えるので、合理性を持った制度であると言える（後述Ⅴ）。しかし、現行法の体系の下では、特別法にもとづく特殊なリスク分配と位置づけられ、預金の払い出しに限定して適用するという解釈が取られている。裁判例には、日本のデビットカードが海外で現地通貨の引き出しに使用された事案に対し、外国通貨の引き出しは、預金の払戻しにも預金を用いた振込にもあたらないとして、偽造カード法の適用を否定したものがある（東京地判平成 29・11・29 金融法務事情 2094 号 78 頁）。

4　オンラインバンキングにおける無権限の支払い指図

オンラインバンキングによる送金や、クレジットカードやデビットカードなどは、銀行預金を決済手段とするキャッシュレス支払いであるが、これらが無権限者によって不正利用された場合、指図に従った送金（振込または振替）であって、預金者への弁済そのものではない。しかし、実務上は、預金の払い出しに準じて民法 478 条の問題になると考えられている[9]。このような考え方は、窓口取引が一般的であった時代に、振り込みの依頼がなされると、いったん預金払い戻しをした上で送金依頼を受け付けるという手続をとっていたことに由来すると言われる[10]。その場合には民法 478 条に関する判例も同じように適用され、支払いシステムの運営者が十分なセキュリティを確保していない場合には、無過失による支払いの実行とは言えず、預金は消滅しないと解されよう。支払いシステムの運営者が取引規定等に置く免責条項も、そのような前提で、有効性を評価され、適用されることとなる。

実際にも、インターネットバンキングを利用していたところ覚えのない振込送金が実行されたと預金者が主張した事案に関する裁判例では、銀行が「システムを、……可能な限度で無権限者による払戻しを排除し得るよう構築し管理していた」と認めた上で、免責規定の有効性が肯定された（［C］東京高判平成 18・７・13 金融法務事情 1785 号 45 頁）。原審の裁判所は、銀行によって取られていたセキュリティ上の措置を、「SSL の技術を用いてお客様番号、ログインパスワード及び暗証番号等を暗号化した上、ログインパスワード及び第２暗証番号については、被告独自の方法で再暗号化してデータベースに格納しており、さらに、暗証番号等の入力を一定回数以上間違えると、それ以上手続が行えなくなる措置や、振込手続が行われた際は、速やかに、届出先のアドレスに電子メールで通知するという措置を講じていただけでなく、本件システムを常時監視していた」と丁寧に認定している（東京高判平成 18・2・13 金融法務事情 1785 号 49 頁）。このような判示は、預金者の主張に応接したという面もあるが、こうしたセキュリティの確保がとられていなかったならば、免責規定を文字どおりには適用しないという趣旨であると考えられる。

5　クレジットカードとデビットカードの不正使用

銀行預金を決済手段とする支払いシステムのうち、クレジットカードやデビットカード（国際カードブランドを付けたいわゆるブランドデビットカード）の場合には、カードの盗難や紛失の場合の不正使用に関して、いったんカード会員の負担とした上で、一定の条

件の下でその支払い義務を免除するという仕組みがとられている。法的な責任とその免除の組み合わせは、偽造カード法が、盗難カードの不正使用リスクについて民法 478 条を適用しつつ、法的な責任とは異なる「補てん」によってリスク負担を調整したことを思わせる。いずれにせよ、これらの支払いシステムにかかわるリスク分配は、仕組みの全体を適用した結果によって定まる。

日本で一般に用いられているカード規約では、カードの盗難・紛失を直ちにカード発行会社（イシュア）に通知した上で警察に届け出ることを条件として、不正使用のリスクは、基本的にイシュアの負担とされている。ただし、カード会員の故意または重過失により盗難・紛失が発生した場合、紛失・盗難の通知を不当に怠ったり遅延した場合の損害、家族等の不正行為による盗難・紛失の場合、会員がカードを他人に提供したことによる盗難・紛失の場合の損害、および盗難・紛失の通知から遡って 61 日以前に発生した不正使用による損害等については、会員の負担となる。物理的なカードの紛失だけではなく、カード番号がオンラインで不正に取得された事故についても、同じリスク分配が適用されている。例外として掲げられた項目は、いずれも、会員の行動によって不正使用の発生や拡大を容易に防止することができる場合であり、会員に対してリスク管理のインセンティヴを与えることに合理性が認められると思われる[11)]。

クレジットカードやデビットカードは銀行預金を決済手段とする支払いシステムであるから、盗難・紛失カードの不正使用は、無権限者による振込指図ととらえることができる。そうだとすれば、カードの不正使用に関する会員規約は民法 478 条に対する特約と位置づけられ、判例法によれば、カード会員にリスクを負担させるためには支払いシステムのセキュリティが確保されている必要があると考えられよう。実際には、クレジットカードやデビットカードのシステムは、国際ブランドの主導の下に高い水準のセキュリティが実装されている。また、磁気ストライプカードの IC チップへの切り替え、大規模小売店舗における IC チップ対応端末の導入、オンラインを含む加盟店のカード番号非保持化といったセキュリティ対策も、経済産業省の支援のもとに、平成 28 年ごろから急速に進められてきた。その結果、少なくとも現在では、一定の場合に不正使用のリスクを会員の負担とする会員規約の有効性が否定されることはないと思われる。

Ⅳ　電子データを決済手段とする支払いシステムの消費者リスク

1　暗号資産（仮想通貨）の無権限者による移動

ビットコインをはじめとする暗号資産は、当初「仮想通貨」と呼ばれ、支払い手段として受領する店舗も現れたことが話題となった。価格の変動が激しいこともあり、最近では、もっぱら投資ないし投機の対象となった印象もあるが、支払い手段として用いられる場合には銀行預金を決済手段としないという点に特徴があるので、ここで取り上げておきたい。

暗号資産には多種多様なものがあると言われ、その取引プラットフォームであるブロックチェーンも、中央管理者が存在しないビットコインのようなシステムばかりではなく、管理者が存在するシステムもある。従って、ひとくくりにして論ずることが適切かという

問題もありそうであるが、以下では、ブロックチェーン上に記録されることが暗号資産に共通の特徴であると考えておこう。なお、多くの消費者は、自らブロックチェーン上のノードになるわけではなく、専門の取引所を通じて暗号資産を入手し、「ウォレット」等と呼ばれる管理アプリの提供を受けて暗号資産を保有・管理することになる[12)]。法制度上は、取引所の運営も、ウォレットの提供も、暗号資産交換業（資金決済法２条７項）として、内閣総理大臣（金融庁）に登録しなければ営むことができない（同法 63 条の２）。

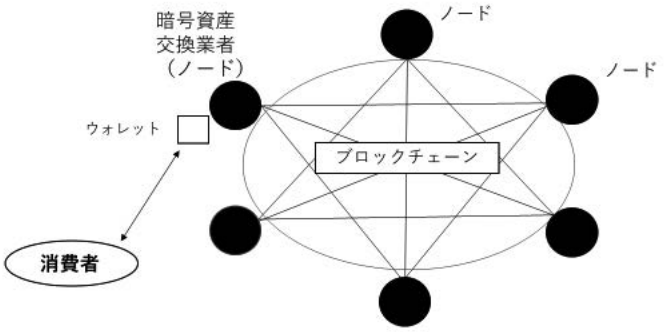

図　暗号資産の取引関係図

（１）　暗号資産交換業者を通じた取引の場合

暗号資産の取引においても、銀行預金を決済手段とするキャッシュレス取引と同様に、消費者の ID（アドレス）やパスワードが盗み出され、不正使用（無権限者による暗号資産の移転指図）が行われるというリスクがある。この状況は、銀行預金の払い出しやオンラインバンキングの不正使用と状況が似ているためか、裁判例は、取引規約に置かれた免責規定が有効と認められるための条件として、暗号資産交換業者がシステムのセキュリティを十分に確保していることを要求する。ビットコインの取引用アカウントに何者かがアクセスし、預託されていた金銭をビットコインに交換した上でアカウント保有者の知らないビットコインアドレス宛てに送付されたという事案で、裁判所は、最高裁の［A］判決を引用して、以下のように判示した（［D］東京地判平成 31・１・25 判例時報 2436 号 68 頁）。

「Y［当時の資金決済法にもとづく仮想通貨交換業者］のビットコインの取引の仕組み（……）からすると、Yは、本件交換及び本件引き出し当時、信義則上、利用者財産の保護のために十分なセキュリティを構築する義務を負っていたと解される……から、当該 API キー及び API シークレットの管理や、当該ユーザーID およびパスワードの管理が

不十分であった場合など、上記義務に違反していると認められる特段の事情がある場合には、本件免責規定は適用されないと解される」

その後、同じように、仮想通貨取引用アカウントのログインパスワード、ワンタイムパスワード及び PIN コードが無権限者によって入力され、仮想通貨の取引が行われた事案でも、仮想通貨交換業者が免責規定の適用を主張したことに対して、利用者の側が、ハッキング対策や不正の疑いがある取引の検知等の仕組みが不十分であったとして免責規定の適用を争った事例がある。裁判所は、不正取引の原因は「X［利用者］のパスワード管理が不十分であったこと」にあると認定した上で、利用者側の主張する仕組みが取られていなかったとしても、現に構築されていた仕組みは不正取引に対する対策としては適切であり、仮想通貨交換業者には不正取引を防止する対策を怠った過失があるとは言えないと判断した（［E］東京地判令和２・３・２金融・商事判例 1598 号 42 頁。控訴審でも、その判断は維持されている。東京高判令和２・12・10 金融・商事判例 1615 号 40 頁）。免責規定を適用するだけではなく、セキュリティの水準が十分であったか否かを検討しているという点で、裁判例は機械払いによる預金払い戻しの事例から一貫しているように思われる。

暗号資産（仮想通貨）の法的性質をめぐっては、①法的権利性を否定する立場、②物権に準ずる権利を認める立場、③民法上の財産権を認める立場、④契約にもとづく存在とする立場などが対立している[13)]。しかし、上記の裁判例の考え方は、そうした議論とは直接のかかわりを持たないと考えられる。この事案における争点は、取引所やウォレット提供者などの暗号資産交換業者と、それらの交換業者を通じて取引を行う消費者との契約関係における免責の問題だからである。取引規約上、暗号資産交換業者は、消費者の指図に従って暗号資産の換金や送付を行う義務を負う。暗号資産に対して物権に準ずる権利が成立するのであれば、それは物権の移転を行う義務であるが、契約によって作り出された無形の「財産的価値」が取引の対象であると考える立場からも、そのような「財産的価値」を享受させる義務を取引契約上の債務として観念することができるであろう。その場合、ID（取引用アドレス）やパスワード、暗証番号（PIN コード）等の合致を、この義務の履行を受領する者の外観と評価し、無権限者がそれらの符号を使用して行う不正取引に民法 478 条を適用すれば、裁判所は、銀行預金の ATM による払い出しやオンラインバンキングの不正利用と同じ考え方をとることになろう。この場合、免責規定は同条の適用に関する特約と位置づけられることになる。しかし、オンラインバンキングについても、民法 478 条の適用範囲が過剰に広げられているという批判がなされてきたところであり、無権限者による指図について表見代理（民法 110 条）を適用し、その中でセキュリティの水準を考慮する（免責規定は表現代理が成立する場合についての特約となる）という構成もあり得るかもしれない。

（２）　直接の取引参加者の場合

これに対して、自らブロックチェーン上のノードとなって暗号資産の取引に参加する主体が、不正なアクセスにより暗号資産を失った場合には、暗号資産の法的な性質論によっ

て、結論が異なり得る。そこまで積極的に関与する主体は、もはや「消費者」とは言えず、業として暗号資産を取り扱う事業者なのではないかとも思われるが、さしあたりその点を措いて、不正取引のリスクを抑止するという観点から分析してみよう。暗号資産に対して物権に準ずる権利を肯定する考え方によれば、不正取引を行った主体自身は暗号資産に対する権利を取得することはなく、その者からの転得者が不正取引について善意無過失であったときに、即時取得によって権利を取得すると考えることになるであろう。そのとき、不正取引の被害者は、即時取得が成立したことの反射的効果として、権利を失うことになる。これは、約束手形の盗難などと同じ帰結である。基本的に、不正取引のリスクは不正なアクセスを受けた被害者が負担することを前提として、転得者に対しても暗号資産の移転経路等に関する調査義務を課す（調査が不十分であれば過失ありとして即時取得を否定する）ものと評価することができよう。

他方で、暗号資産を、取引当事者の契約によって作り出された財産的な価値であると見た場合には、不正に取得した者やその者からの転得者を含め、取引記録上で暗号資産を保有するとされている者に権利行使を認めることになるのではないかと思われる。もちろん、不正取得者に対しては不法行為にもとづく損害賠償請求や不当利得の返還請求が可能になり、転得者に対しても、事実関係によっては同様の請求が成り立つ可能性があるが、それは、いったん成立した暗号資産の取引を解消するのではなく、不正取得者から被害者に対する暗号資産の新たな移転や、それに代わる金銭の支払いによって処理されることになる[14]。このような取り扱いは、「占有と所有の一致」を原則とする金銭と同じである[15]。不正取引のリスクは全面的に被害者が負担することになるため、不正アクセスを防ぐための行動をとるインセンティヴが、暗号資産の現在の保有者（潜在的な被害者）に対して与えられる。

約束手形の場合、かつては手形の流通保護が強調され、善意取得の成立を認めることが肯定的に評価されていたが、平成期の裁判例には、手形取得者にかなり高度の調査義務を課し、振出人名などに照らして流通経路が不自然な場合に、所持人が手形を適法に入手したことの確認を怠った場合には、重過失ありとして善意取得を否定するものも少なくない（東京地判平成 11・６・30 判例タイムズ 1015 号 238 頁、東京高判平成 12・８・17 金融・商事判例 1109 号 51 頁など）。そのような裁判例は、優良企業が振り出す約束手形は裏書を繰り返すことなく金融機関に割り引かれるという取引実態を背景として、それとは異なる経路で流通する約束手形を取得する者に、盗難手形の流通というリスクを抑止するインセンティヴを与えるものと言える。これと比較するとき、暗号資産の流通プラットフォームであるブロックチェーンは、たしかに、過去の取引を改竄不能な形で記録する仕組みではあるが、そこに言う記録は、約束手形の裏書などとは違い、会社の商号や所在地の記載から商業登記と突き合わせて不審な取引の介在を調査する手がかりになるという性質のものではない。そのことと、ブロックチェーン上にノードを持って取引に参加するような当事者は、消費者というよりも専門的な投資家に近いと考えられることとを併せて考慮すれば、物権に準じた処理ではなく、占有と所有が一致する金銭に等しい扱いとする方が、合理的なのではないかと思われる。

２　電子マネーの盗難と無権限利用

（１）　IC カード型電子マネー

交通系など、IC カードに電子データを記録するタイプの電子マネーの場合、基本的に、カードの占有によって電子マネーの使用権原が確認される。その結果として、他人の IC カードを入手した者が電子マネーを使うと、それは有効な取引として処理される。電子マネーの発行主体が加盟店から電子データを買いとる際に、不正に入手された IC カードから移転された電子データかどうかを区別することは技術的に不可能だからである。もちろん、IC カードという有体物（動産）に対して元の所有者が持つ所有権は、即時取得が成立するまで失われることはないから、IC カードを盗まれたり紛失したりした者は、そのカードの返還を求めることができる。またカードを入手した者が無権限で使用した電子マネー相当額も、不法行為による損害賠償請求または不当利得の返還請求の対象になるが、それは電子マネーのシステムの外で行われ、システム上で電子マネーが返還されるわけではない。

これは、現金と同じく占有と所有が一致する仕組みであり、仮想通貨に関して述べたところと同様に、IC カードを所持する者に盗難や紛失のリスクを負担させ、それを回避するように注意させるシステムであると言える。有体物である IC カードの管理に最も適した立場にある者は、現在の所持者であるから、紛失や盗難に気づいたら電子マネー発行者に通知することを含め、消費者にリスク回避の行動をとらせることには合理性が認められよう。とはいえ、他のキャッシュレス取引と同様に考えるなら、IC カード型電子マネーの場合も、消費者にリスクを負担させる前提として、システムのセキュリティが十分でなければならないであろう。

IC カード型電子マネーのセキュリティは、①チャージが可能な金額の上限設定、②カードの物理的な占有を失うことなくデータが抜き取られるリスクの排除（IC カードの耐タンパ性）、そして③盗難、紛失等の場合に利用を停止する仕組みの整備、などによって構成される。不正使用のリスクを排除する効果はこれらの組み合わせを総合して実現されるので、たとえば、チャージ金額の上限（①）が低く抑えられている場合には、プライバシーを重視して利用者の追跡をさせない代わりに利用停止の仕組み（③）を持たないという無記名のカードがあってもよいであろう。しかし、オートチャージによって無制限に不正使用が進む可能性がある場合には、利用停止の仕組みが存在し、かつ、そのために消費者がとるべき行動が周知されている必要があると考えられる。

近年では、電子マネーをスマートフォン上のアプリとして提供し、スマートフォンの端末を媒体（デバイス）として使用するタイプのサービスも普及してきたが、以上の考え方は異ならない。ただし、消費者は、スマートフォンを「携帯電話」として認識しがちであるため、通信キャリア（通話サービスの提供事業者）への連絡によって安心してしまい、電子マネーの不正使用を差し止める機会を逸してしまうという危険がある。銀行預金の払い出しに関する判例に従うなら、そうしたリスクの周知も、セキュリティの一環であり、電子マネーの発行者が免責を受けるための前提とされるべきであろう。実際にも、スマートフォン上の電子マネーアプリにオートチャージが設定されていた事案において、電子マネーの発行主体は「登録携帯電話の紛失等が生じた場合に、本件サービスの不正利用を防

止するため、登録会員がとるべき措置について適切に約款等で規定し、これを周知する注意義務がある」とした裁判例がある（［F］東京高判平成 29・１・18 判例時報 2356 号 121 頁）。

（２）　サーバ型電子マネー

IC カード型と並んで普及している電子マネーに、サーバ型と呼ばれるものがある。これは、電子マネーの保有者と残高を電子マネー発行者のコンピュータ・サーバ上で管理し、記録上の保有者から支払いの指図が行われた場合に、指定された相手方および金額で資金移動を行うというものである。保有者の特定は、プラスチックカード上の磁気テープに記録された情報によって行われるもの（ファストフード店などでカードを発行するタイプのサーバ型電子マネー）もあれば、文字列などの符号によって行われるもの（利用者が符号を記載した紙のカードを購入したり、符号をプリントアウトしたりして利用するタイプのサーバ型電子マネー）もある。これらのサーバ型電子マネーでも、電子マネー発行者と加盟店の間では銀行間の振込を利用した資金移動が行われるが、利用者は、現金によるチャージ（プラスチックカードを提示した入金操作、文字列などを記載した紙のカードの購入等）を行う場合もあり、利用者の銀行預金から直接的な資金移動が行われる仕組みとはなっていない。

サーバ型電子マネーでも、IC カード型の電子マネーと同じように、プラスチックカードや文字列などの符号を不正に入手した無権限者がそれを使用した場合、電子マネーが消滅するとされている。プラスチックカードが電子マネー保有者の特定に用いられている場合は、物理的な媒体（デバイス）が配布され、それを利用者が管理しているという点で、IC カード型電子マネーと同じリスク分配を適用してよいであろう。しかし、文字列などの符号によって管理されるサーバ型電子マネーの場合は、不正使用のリスクを回避する行動をもっぱら利用者に期待することはできないのではないか。いったん符号がサーバに登録されると、サーバのセキュリティが不十分であれば、消費者側にまったく原因がなくとも不正使用が発生しうる。また、サーバを運用する従業員の不正行為も、利用者には管理しえないリスクである。ここでも、電子マネー発行主体が（従業員の管理など人的な要素を含めた）セキュリティを十分な水準で確保することが、不正使用のリスクを利用者に負担させる上での前提になると考えられる。

前述したとおり（Ⅰ　2）、QR コード支払いなどの新しいキャッシュレス支払いは、利用形態によってサーバ型電子マネー（資金決済法上の前払式支払手段）となる場合がある。このときは、仮にクレジットカードからチャージが行われたとしても、クレジットカードの会員規約ではなく、キャッシュレス支払いの利用規約にもとづいてリスクの分配が行われることになる。そして、そうした利用規約の内容には、いっさいの限定なく利用者にリスクを負担させるものから、コード支払い事業者の態様（故意・重過失など）や利用者の態様（パスワード管理等）を条件としたリスクの分配を定めるもの、クレジットカードの会員規約に類似した補償制度を設けるものなど、さまざまな事例があるようである[16]。しかし、どのような規定を置いた場合でも、利用者にリスクの負担を求める際には、システ

ムについて十分な水準のセキュリティが確保されていることが前提となるべきであるし、裁判で争われれば、おそらくそのように判断されるであろう。

Ⅴ　無権限取引のまとめ

キャッシュレス取引におけるリスクの分配は、支払い手段によって、少しずつ異なっている。しかし、それは支払い手段ごとの特徴に合わせてルールが調整されているというよりは、利用規約（とくに免責条項）が作られてきた経緯の違いや、判例・特別法などによる修正などが重なった偶然の結果という側面が大きいように思われる。金融審議会でも、「事業者・利用者双方が無権限取引〔本稿でいう「不正使用」――引用者〕を防止するインセンティブを持つこととなるような、統一的なルールの整備」を提案する意見が述べられたと報告されている[17]。そこで改めて、支払いシステム全体に対するリスクの抑制という観点から、リスク分配が持つ効果を整理してみよう。

まず、キャッシュレス支払いにおいては、なんらかの識別標識によって支払いを行う主体（利用者）を特定しなければならない。識別標識は、カードや端末などの有体物と暗証番号などを組み合わせる場合と、ID とパスワードなど複数の符号の組み合わせから構成される場合とがある。これらの識別標識については、支払い主体自身による管理と、支払いシステムの側の管理の双方が必要になる。識別標識を不用意に他人に使わせれば不正使用の原因となりうるし、極端な場合には、利用者が不正使用者と共謀してシステムを悪用する場合もある。他方で、識別標識を保存しているサーバが攻撃されたり、通信中の標識を読み取られたりするリスクは、システム運営者の側でしか抑止できない。この双方に対してリスク抑止のインセンティヴを与えるためには、リスクの分配に際して、双方の過失ないしは帰責事由を考慮することが望ましい。

銀行預金の機械による払い出しに関し、対面取引による払い出しの延長で民法 478 条を適用する考え方に対して、多くの学説が批判をしてきた理由は、この点にある。民法 478 条は、債権者側（銀行預金を決済手段とするキャッシュレス支払いのシステム運営者側）の過失のみを考慮する規定とされているからである。しかし、判例が、同条にいう過失の内容としてシステムの安全性を読み込んだことにより、状況は変化しているように思われる。要求されるシステムの安全性をきわめて高い水準に設定すれば、預金者側に過失（帰責事由）がないにもかかわらず不正使用が発生するようなシステムは安全性を欠いていたと判断することも可能であろう[18]。その意味で、現在の判例法の下では、支払いシステムの運営者側に求められる安全性の水準が本質的な意味を持つとも言える。

言うまでもなく、システムのセキュリティは無償で実現できるわけではない。そして、そのコストは、結局のところ支払いシステムの利用者全体が広く薄く負担することになる（価格の転嫁がどの程度行われるかはサービス市場の競争の度合いによるので、常に全額が転嫁できるわけではない）。そうだとすれば、システムに高度なセキュリティを求めることと、不正使用の被害者に対して補償などの形で救済を与えることとは、利用者から見れば機能的には違いがないとも言える。その相違は、リスクの抑止にコストをかけ、それを

利用者全体で負担することか、リスクを抑止できずに発生した被害を補償し、その原資を利用者全体に転嫁するかの違いにすぎないからである。そして、リスクの抑止に必要なコストとそれによって防止される不正使用の被害規模を比較し、最適なセキュリティの水準を決定できる立場にあるのは、支払いシステムの運営者である。このように考えるならば、支払い主体に帰責事由が認められる場合を除いて、不正使用の被害はシステム全体による負担の下に補償されることが望ましいと言える。すなわち、偽造カード法やクレジットカードの会員規約が定めるリスクの分配は、基本的に正しい方向を示していると評価することができる。

ところで、実務上、支払いシステムには複数の主体が関与しており、その関与の仕方もシステムによって一様ではない。そのことを前提としたとき、不正使用のリスクを引き受け、システムのセキュリティ確保に尽力すべき「支払いシステムの運営者」とは、具体的にはどの事業者を差すのかという点が疑問になるかもしれない。不正使用の問題が、基本的には支払い主体の特定における不正であることを考えると、第一義的には、支払い主体を把握している事業者がこれにあたると言うべきであろう。クレジットカードやデビットカードのイシュアがこれに該当する。これに加えて、資金移動のシステム全体のセキュリティに関しては、カードの国際ブランドなど、そうしたシステムを構築し、提供している主体にもリスク抑止のインセンティヴが機能するような仕組みが望ましいと言える。現状では、そうした決済システムが寡占化しており、かつ、いずれのシステム運営者もセキュリティの向上に努めているため問題が顕在化していないが、たとえば、各種の暗号資産が乱立しつつ、支払い手段として広く普及していくような状況が訪れるならば、システム全体のセキュリティ確保をどの当事者の責任とするかについて検討する必要が生ずるであろう。

Ⅵ　結語

キャッシュレス社会の実現という政策課題が掲げられる中で、昨今、新しい支払い手段が次々と出現しているが、それらを利用する消費者にとってのリスクについて考えることは、政策の実現を図る上で重要なカギになる。未知のリスクが大きいと認識すれば、消費者は、リスクを熟知している現金取引の方を選択するであろうからである。そして、支払いシステムのリスクを全体として抑制していくためには、リスクを効果的に抑止できる立場にある当事者に、適切な行動をとるためのインセンティヴが与えられなければならない。支払いシステムの下におけるリスク分配のルールは、そのような効果が認められる場合に、効率的なものと評価することができる。

現金取引と異なり、新しい支払い手段は、システムの中で利用されるため、リスクの抑制のためには、システムのセキュリティが重要な役割を果たす。幸いなことに、銀行預金の機械（当初は CD 機、後には ATM）による払い出しが可能になった頃から、システムの安全性を当事者の注意義務に位置づける学説が提唱され、判例によって取り入れられていった。その結果、現在では、銀行預金を決済手段としない暗号資産の取引においても、免責

条項を有効と認める前提としてシステムの安全性が要求されるようになっている。支払いシステムの安全性は、いまや、民法 478 条やその特約としての約款条項を離れ、支払いシステム運営者の免責一般に妥当する法理となった感がある。

他方で、システムの安全性に対するインセンティヴをどの当事者に与えるかという点については、なお確立した考え方がないように思われる。支払い主体にも、自己を識別する符号や端末の管理を通じたリスクの抑制が求められる反面で、システムが高度化、複雑化すればするほど、そのセキュリティを確保することは、もっぱらシステム運営者に期待されるようになる。セキュリティの確保に必要なコストとリスク抑制の効果を均衡させる水準は、システム運営者が最も適切に判断できるので、支払い主体に帰責事由がある場合を除き、事故による損失はシステム運営者が引き受けた上で、システムの利用コストとして利用者全体に負担させることが望ましいと考えられる。そのようなリスクの分配は、預金の機械払いに適用される偽造カード法やクレジットカードの会員規約では採用され、一部のキャッシュレス取引の規約にも広がってきているものの、新しい支払い手段に共通した考え方と認められるには至っていないようである。

より大きな視野に立つと、FinTech と呼ばれる新しい金融技術に関して、「市場に対する信頼」「技術革新（イノベーション）の促進」「ルールの簡明さ」という三つの政策目標があり、相互に対立する（いわゆるトリレンマになる）と指摘する見解がある[19)]。消費者にとってのリスクが適切に管理されることは「市場に対する信頼」の重要な要素をなす。今後、新しい支払い手段に関して、他の二つの要素とのバランスをも考慮しつつ、適切なリスク管理を実現するようなルールの形成が期待される。

［注］

1）消費者の意識については、唯根妙子「キャッシュレス推進に伴う消費者トラブル～実態調査等を通じて対策を考える～」法とコンピュータ 38 号〔2020〕15 頁。

2） 支払いと決済の仕組みを区別して論ずる必要性については、小塚荘一郎＝森田果『支払決済法』［第３版］〔商事法務、2019〕15 頁以下参照。

3）最判昭和 29・11・５刑集８巻 11 号 1675 頁、最判昭和 39・１・24 判例時報 365 号 26 頁。理論的な背景などについて、能見善久「金銭の法律上の地位」『民法講座　別巻１』〔有斐閣、1990〕101 頁、古市峰子「現金、金銭に関する法的一考察」金融研究 14 巻４号〔1995〕101 頁。

4）林良平「CD 取引の法的構造」金融法務事情 739 号〔1974〕６頁、９頁。

5）その後に出された［B］判決をふまえれば、民法 478 条にいう債務者の無過失要件を免責条項の解釈に持ち込んだものと見ることもできるが、この判決が出された当時は、問題となった免責条項が民法 478 条を前提とした契約条項であるのか否かについても見解は分かれていたので（長尾治助・［A］判決評釈・私法判例リマークス９号〔1994〕47 頁、48 頁、山本豊・［A］判決評釈・金融法務事情 1396 号〔1994〕７頁、８～９頁などを参照）、そのような趣旨であったか否かも明確ではない。

6） 我妻榮『新訂債権総論』〔岩波書店、1964〕280 頁、中田裕康『債権総論［第４版］』〔岩波書店、2020〕391～393 頁。このような理解を批判する学説も有力である。潮見佳男『新債権総論』〔信山社、2017〕213～217 頁参照。

7）全国銀行協会「偽造・盗難キャッシュカードに関する預金者保護の申し合わせ」（平成 17 年 10 月６日）＜https://www.zenginkyo.or.jp/fileadmin/res/news/news171006_2.pdf＞。
8）「偽造・盗難キャッシュカードに関する預金者保護の申し合わせ」が、重過失の有無を判断する際等に、「預金者の年齢（特に高齢者など）、心身の状況等に十分配慮した対応を行うこと」を求めていることに照らせば、そうした状況が理由となって他人に暗証番号を知らせたりキャッシュカードを渡したりした事案では、裁判所も重過失の認定には慎重になるであろう。
9）中舎寛樹・［C］判決評釈・金融法務事情 1812 号〔2007〕11 頁。
10）岩原紳作『電子決済と法』〔有斐閣、2003〕184～185 頁。
11）裁判例にも、会員規約のこうした規定を全体としてみれば、合理性があると述べるものがある（東京地判平成５・10・18 判例時報 1488 号 122 頁）。
12）道垣内弘人「仮想通貨の法的性質――担保物としての適格性――」『社会の発展と民法学・近江幸治先生古稀記念論文集〔上巻〕』〔成文堂、2019〕489 頁
13）これらの学説の対立点については、加毛明「仮想通貨の私法上の法的性質――ビットコインのプログラム・コードとその法的評価」『仮想通貨に関する私法上・監督法上の諸問題の検討』〔2019 年、金融法務研究会〕１頁、16 頁以下、得津晶「日本法における仮想通貨の法的諸問題：金銭・所有権・リヴァイアサン」法学 81 巻２号〔2017〕83 頁などを参照。それぞれの学説の出所についても、両論文に網羅されている。
14）加毛・前掲〔註 13〕・29 頁。
15）金銭についても、「占有と所有が一致する」からといって、盗んだり騙し取ったりした者に対する不当利得返還請求権が排除されるわけではない（最判昭和 49・９・26 民集 28 巻６号 1243 頁）。
16）一般社団法人キャッシュレス推進協議会『コード決済における不正利用に関する責任分担・補償等についての規定事例集（利用者向け利用規約）』〔2019〕＜https://www.paymentsjapan.or.jp/news/20190830-user-compensation/＞。
17）『金融審議会　決済法制及び金融サービス仲介法制に関するワーキング・グループ報告』〔2019〕15 頁脚注 29。
18）尾島茂樹・［B］判決評釈・判例評論 541 号〔2004〕２頁、６頁も、「事実上、〔銀行と預金者の〕両者がまったく無過失ということがあり得るだろうか」という疑問を提示する。ただし、裁判例がそうした高い水準のセキュリティを要求していたと言えるかは、また別の問題である。［A］判決が「特段の事情」を否定したことに対して、昭和 56 年当時でもゼロ化されていないキャッシュカードの危険性は広く認識されており、また国際的に見ても危険なシステムであったとして、批判する見解がある（岩原・前掲書〔註 10〕・176 頁）。
19）Chris Brummer & Yesha Yadav, ‘Fintech and the Innovation Trilemma’, (2019) 197 *Georgetown Law Journal* 235.